Remarks:

Applicants have read and considered the Office Action dated March 17, 2006 and the references cited therein. Claims 13, 17 and 21 have been amended. Claims 13-24 are currently pending.

In the Action, claims 13, 17 and 21 were provisionally rejected under the doctrine of obviousness-type double patenting as being unpatentable over claims 19, 27, 28 and 29 of copending Application No. 10/089,662 in view of IBM Technical Disclosure Bulletin v36 n10 10-93 p413-416. Applicants assert that the claims are patentably distinct from the claims of copending Application No. 10/089,662 in light of the IBM Technical Disclosure Bulletin. Applicants assert that the cryptographic system from 10/089,662 differs on a basic level. The CRYPTOGRAPHIC SYSTEM of 10/889,662 requires that at least one base member g_i is a quadratic residue of the ring of integers module n. Such a system with the requirement of the base member being a quadratic residue of the ring of integers modulus n changes the mathematical features of the system. Such basic differences are patentably distinct.

Moreover, Applicants assert that the claims have been amended and further distinguish over the prior art. Applicants assert that the selection of base numbers wherein each base member is an integer greater than 1 and is a non-quadratic residue of the ring of integers module n, clearly distinguishes over the copending application and the IBM Technical Disclosure Bulletin. Applicants assert that the present application is patentably distinct from the copending application. Applicants request that the obviousness-type double patenting rejection be withdrawn.

In addition, claims 13, 17 and 21 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 19-28 of copending Application No. 09/889,918 in view of the IBM Technical Disclosure Bulletin. Applicants assert that the '918 application and this application relate to complementary, but

distinct aspects of a cryptographic system. Applicants assert that the different claims are patentably distinct. Moreover, the claims of the present invention have been amended and Applicants note that the claims of the '918 application have also been recently amended and both applications are believed to further distinguish from one another. Applicants assert that the claims as submitted are patentably distinct over the pending claims of the '918 application. Applicants request that the obviousness-type double patenting rejection be withdrawn.

Claims 13, 17 and 21 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 10/089,646. Applicants assert that the pending claims as submitted, are patentably distinct over the '646 application and the IBM Technical Disclosure Bulletin. The present application deals with prime factors modulus N which are congruent to 3 mod 4 ($p_i \equiv 3 \bmod 4$). Moreover, the present application also relates to prime factors modulus n which are congruent to one mod 4 ($p_j \equiv 1 \bmod 4$). Applicants also note that the claims have been amended and further distinguish over the '646 application and the IBM Technical Disclosure Bulletin as the claims recite selecting M base numbers $g_1, g_2, \ldots, g_m$ wherein each base number is an integer greater than 1 and is a non-quadratic residue of the ring of integers modulo n. Applicants assert that neither the '646 application and IBM Technical Disclosure Bulletin neither teach nor suggest at least this feature. Applicants assert that the claims are patentably distinct over the combination of cited references. Applicants request that the provisional obviousness-type double patenting rejection be withdrawn.

Claims 13, 17 and 21 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 29 of copending Application No. 10/471,884 in view of the IBM Technical Disclosure Bulleting. Applicants assert that the '884 application deals with the specific application of public-key cryptography. The '884 application asserts that it is possible to choose a small module, on the condition that precautions have been taken relative to security level. The application recites that "said public

module *n* being small relative to the private signature key and such that it cannot be factorized by a computer having state of the art computing power in a time as short as the duration of the session." This teaches away from the system of the present invention and differs from the present invention in a patentably distinct way. In addition, Applicants assert that the claims have been amended as discussed above. Moreover, Applicants assert that the claims recite an invention that is neither shown nor suggested and that the claims patentably distinguish over the '884 application and the IBM Technical Disclosure Bulletin. Applicants request that the obviousness-type double patenting rejection therefore be withdrawn.

Claims 13-24 contain allowable subject matter and would be allowed upon overcoming the provisional double patenting rejection. Applicants thank the Examiner for the indication of allowable subject matter. However, Applicants note that the claims have been amended and overcome the double patenting rejections. In addition, claims 14-16, 18-20 and 22-24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicants thank the Examiner for the indication of allowable subject matter. However, as discussed above, Applicants assert that the base claims overcome the double patenting rejections and are in condition for allowance. Applicants assert that all claims are now in condition for allowance.

A speedy and favorable action in the form of a Notice of Allowance is hereby solicited. If the Examiner feels that a telephone interview may be helpful in this matter, please contact Applicant's representative at (612) 336-4728.

23552
PATENT TRADEMARK

Respectfully submitted,

MERCHANT & GOULD P.C.

Dated: 8/17/06

By: _____
Gregory A. Sebald
Reg. No. 33,280
GAS/km